August 1997

Singular and plural non-deterministic parameters

Sigurd Meldal
San Jose State University, sigurd.meldal@sjsu.edu

M. A. Walicki

ND ARUN SHARMA

logy, Cognition, 2 (1973), pp. 131–146.
s., *Proc. 2nd Annual Workshop on Com-*
San Mateo, CA, 1989.
nctions, J. Symbolic Logic, 23 (1958), pp.

ective Computability, McGraw–Hill, New
1987.
f effective program synthesis-learning by
Sci., 215 (1986), pp. 219–225.
ram synthesis, J. Assoc. Comput. Mach.,

nference, part I, Inform. and Control, 7

ference, part II, Inform. and Control, 7

th Annual Workshop on Computational
CA, 1991.

SIAM J. COMPUT.
Vol. 26, No. 4, pp. 991–1005, August 1997

005

SINGULAR AND PLURAL NONDETERMINISTIC PARAMETERS*

MICHAL WALICKI† AND SIGURD MELDAL†

Abstract. The article defines algebraic semantics of singular (call-time-choice) and plural (run-time-choice) nondeterministic parameter passing and presents a specification language in which operations with both kinds of parameters can be defined simultaneously. Sound and complete calculi for both semantics are introduced. We study the relations between the two semantics and point out that axioms for operations with plural arguments may be considered as axiom schemata for operations with singular arguments.

Key words. algebraic specification, many-sorted algebra, nondeterminism, sequent calculus

AMS subject classifications. 68Q65, 68Q60, 68Q10, 68Q55, 03B60, 08A70

PII. S00975397264317

1. Introduction.

The notion of *nondeterminism* arises naturally in describing concurrent systems. Various approaches to the theory and specification of such systems, for instance, CCS [16], CSP [9], process algebras [1], and event structures [26], include the phenomenon of nondeterminism. But nondeterminism is also a natural concept in describing sequential programs, either as a means of indicating a "don't care" attitude as to which among a number of computational paths will actually be utilized in a particular computation (e.g., [3]) or as a means of increasing the level of abstraction [14, 25]. The present work proceeds from the theory of *algebraic specifications* [4, 27] and generalizes the theory so that it can be applied to describing nondeterministic operations.

In deterministic programming the distinction between call-by-value and call-by-name semantics of parameter passing is well known. The former corresponds to the situation where the actual parameters to function calls are evaluated and passed as values. The latter allows parameters which are function expressions, passed by a kind of Algol copy rule [21], and which are evaluated whenever a need for their value arises. Thus call-by-name will terminate in many cases when the value of a function may be determined without looking at (some of) the actual parameters, i.e., even if these parameters are undefined. Call-by-value will, in such cases, always lead to undefined result of the call. Nevertheless, the call-by-value semantics is usually preferred in the actual programming languages since it leads to clearer and more tractable programs.

Following [20], we call the nondeterministic counterparts of these two notions *singular* (call-by-value) and *plural* (call-by-name) parameter passing. Other names applied to this, or closely related distinction, are *call-time-choice* vs. *run-time-choice* [2, 8] or *inside-out* (IO) vs. *outside-in* (OI), which reflect the substitution order corresponding to the respective semantics [5, 6]. In the context where one allows nondeterministic parameters, the difference between the two semantics becomes quite apparent even without looking at their termination properties. Let us suppose that

*Received by the editors March 9, 1994; accepted for publication (in revised form) August 7, 1995. The research of the first author was partially supported by the Architectural Abstraction project under NFR (Norway), the CEC under ESPRIT-II Basic Research Working Group 6112 COMPASS, DARPA under ONR contracts N00014-92-J-1928 and N00014-93-1-1335, and Air Force Office of Scientific Research grant AFOSR-91-0354.

http://www.siam.org/journals/sicomp/26-4/26431.html

†Department of Informatics, University of Bergen, HiB, 5020 Bergen, Norway (michal.walicki@ii.uib.no, sigurd.meldal@ii.uib.no).

we have defined operation $g(x)$ as "**if** $x = 0$ **then** a **else** (**if** $x = 0$ **then** b **else** c)" and that we have a nondeterministic choice operation $\sqcup$ returning an arbitrary element from the argument set. The singular interpretation will satisfy the formula ϕ: $g(x) = (\textbf{if } x = 0 \textbf{ then } a \textbf{ else } c)$, whereas the plural interpretation need not satisfy this formula. For instance, under the singular interpretation $g(\sqcup.\{0,1\})$ will yield either a or c, whereas the set of possible results of $g(\sqcup.\{0,1\})$ under the plural interpretation will be $\{a,b,c\}$. (Notice that in a deterministic environment both semantics would yield the same results.) The fact that the difference between the two semantics occurs already in very trivial examples of terminating nondeterministic operations motivates our investigation.

We discuss the distinction between the singular and the plural passing of nondeterministic parameters in the context of algebraic semantics, focusing on the associated reasoning systems. The singular semantics is given by *multialgebras*, that is, algebras where functions are set valued and where these values correspond to the sets of possible results returned by nondeterministic operations. Thus, if f is a nondeterministic operation, $f(t)$ will denote the set of possible results returned by f when applied to t. We introduce the calculus NEQ which is sound and complete with respect to this semantics.

Although terms may denote sets, the variables in the language range only over individuals. This is motivated by the interest in describing unique results returned by each particular application of an operation (execution of the program). It gives us the possibility of writing instead of a formula $\mathbf{\Phi}(f(t))$, which expresses something about the whole set of possible results of $f(t)$, the formula corresponding to $x \in f(t) \Rightarrow \mathbf{\Phi}(x)$, which express something about each particular result x returned by $f(t)$. Unfortunately, this poses the main problem of reasoning in the context of nondeterminism—the lack of general substitutivity. From the fact that $h(x)$ is deterministic (for each x has a unique value) we cannot conclude that so is $h(t)$ for an arbitrary term t. If t is nondeterministic, $h(t)$ may have several possible results. The calculus NEQ is designed so that it appropriately restricts the substitution of terms for singular variables.

Although operations in multialgebras are set valued, their carriers are usual sets. Thus operations map individuals to sets. This is not sufficient to model plural arguments. Such arguments can be understood as sets being passed to the operation. The fact that, under plural interpretation, $g(x)$ as defined above need not satisfy ϕ results from the two occurrences of x in the body of g. Each of these occurrences corresponds to a repeated application of choice from the argument set x, that is, potentially, to a different value. In order to model such operations we take as the carrier of the algebra a (subset of the) power set—operations map sets to sets. In this way we obtain *power algebra* semantics. The extension of the semantics is reflected at the syntactic level by introduction of *plural variables* ranging over sets rather than over individuals. The sound and complete extension of NEQ is obtained by adding one new rule which allows for usual substitution of arbitrary terms for plural variables.

The structure of the paper is as follows. In sections 2 and 3 we introduce the language for specifying nondeterministic operations and explain the intuition behind its main features. In section 4 we define *multialgebraic* semantics for singular specifications and introduce a sound and complete calculus for such specifications. In section 5 the semantics is generalized to *power algebras* capable of modeling plural parameters, and the sound and complete extension of the calculus is obtained by introducing one additional rule. A comparison of both semantics in section 6 is guided

by the similarity of the respectiv
and power models which may se
also highlight the increased comp
problems with intuitive understa

Proofs of the theorems are m
of the results from [24] where the

2. The specification lang

signature Σ is a pair $(\mathbf{S},\mathbf{F})$ of so
result sorts in $\mathbf{S}$). The set of ter
by $W_{\Sigma,X}$. We always assume tha
S, S^{W_Σ}, is not empty.[1]

Π is a set of sequents of atom
left-hand side (LHS) of $\mapsto$ is calle
consequent, and both are to be u
ing and multiplicity of the atomic
antecedent or consequent to be en
sequent with exactly one formula
and a Horn formula with empty
sequent).

All variables occurring in a s
whole sequent. A sequent is satis
the antecedents is false or one of
$a_1 \wedge \cdots \wedge a_n \Rightarrow e_1 \vee \cdots \vee e_m$ is va

For any term (formula set of
ξ. If the variable set is not menti
that x is a variable.

An atomic formula in the con
$t \prec s$, of terms t, $s \in W_{\Sigma,X}$. An a
be interpreted as nonempty inters
For a given specification SP = (Σ,
signature Σ.

The above conventions will b
tween the singular and the plura
reflected in the notation by the su
the set of plural variables in a ter
SP*, the corresponding extension

3. A note on the intuitive

interprets specifications in some f
tic) operations correspond to *set-*
is interpreted as a set of *possibiliti*
sponding operation. We, on the o
facts, i.e., facts which have to hol
This is achieved by interpreting t
Every two syntactic occurrences o
of t. For nondeterministic terms th

[1] This restriction is motivated by th
requires additional mechanisms (explicit
that a similar solution can be applied in

by the similarity of the respective calculi. We identify the subclasses of multimodels and power models which may serve as equivalent semantics of one specification. We also highlight the increased complexity of the power algebra semantics reflecting the problems with intuitive understanding of plural arguments.

Proofs of the theorems are merely indicated in this presentation. It reports some of the results from [24] where the full proofs and other details can be found.

2. The specification language. A specification is a pair (Σ, Π), where the signature Σ is a pair $(\mathbf{S},\mathbf{F})$ of sorts $\mathbf{S}$ and operation symbols $\mathbf{F}$ (with argument and result sorts in $\mathbf{S}$). The set of terms over a signature Σ and variable set X is denoted by $W_{\Sigma,X}$. We always assume that, for every sort S, the set of ground words of sort S, S^{W_Σ}, is not empty.[1]

Π is a set of sequents of atomic formulas written as $a_1, \ldots, a_n \mapsto e_1, \ldots, e_m$. The left-hand side (LHS) of $\mapsto$ is called the *antecedent* and the right-hand side (RHS) the *consequent*, and both are to be understood as sets of atomic formulas (i.e., the ordering and multiplicity of the atomic formulas do not matter). In general, we allow either antecedent or consequent to be empty, though $\emptyset$ is usually dropped in the notation. A sequent with exactly one formula in the consequent ($m = 1$) is called a *Horn formula*, and a Horn formula with empty antecedent ($n = 0$) is a *simple formula* (or a *simple sequent*).

All variables occurring in a sequent are implicitly universally quantified over the whole sequent. A sequent is satisfied if, for every assignment to the variables, one of the antecedents is false or one of the consequents is true (it is valid iff the formula $a_1 \wedge \cdots \wedge a_n \Rightarrow e_1 \vee \cdots \vee e_m$ is valid).

For any term (formula set of formulas) ξ, $\mathcal{V}[\xi]$ will denote the set of variables in ξ. If the variable set is not mentioned explicitly, we may also write $x \in \mathcal{V}$ to indicate that x is a variable.

An atomic formula in the consequent is either an *equation*, $t = s$, or an *inclusion*, $t \prec s$, of terms $t, s \in W_{\Sigma,X}$. An atomic formula in the antecedent, written $t \frown s$, will be interpreted as nonempty intersection of the (result) sets corresponding to t and s. For a given specification $\mathrm{SP} = (\Sigma, \Pi)$, $\mathcal{L}(\mathrm{SP})$ will denote the above language over the signature Σ.

The above conventions will be used throughout the paper. The distinction between the singular and the plural parameters (introduced in the section 5) will be reflected in the notation by the superscript *: a plural variable will be denoted by x^*, the set of plural variables in a term t by $\mathcal{V}^*[t]$, a specification with plural arguments SP^*, the corresponding extension of the language $\mathcal{L}$ by $\mathcal{L}^*$, etc.

3. A note on the intuitive interpretation. Multialgebraic semantics [10, 13] interprets specifications in some form of power structures where the (nondeterministic) operations correspond to *set-valued functions*. This means that a (ground) term is interpreted as a set of *possibilities*; it denotes the set of *possible* results of the corresponding operation. We, on the other hand, want our formulas to express *necessary* facts, i.e., facts which have to hold in *every evaluation* of a program (specification). This is achieved by interpreting terms as *applications* of the respective operations. Every two syntactic occurrences of a term t will refer to *possibly distinct* applications of t. For nondeterministic terms this means that they may denote two distinct values.

[1] This restriction is motivated by the fact (pointed out in [7]) that admitting empty carriers requires additional mechanisms (explicit quantification) in order to obtain sound logic. We conjecture that a similar solution can be applied in our case.

Typically, equality is interpreted in a multialgebra as *set equality* [13, 23, 12]. For instance, the formula $\mapsto t = s$ means that *the sets corresponding to all possible results* of the operations t and s are equal. This gives a model which is mathematically plausible but which does not correspond to our operational intuition. The (set) equality $\mapsto t = s$ does not guarantee that the result returned by some particular application of t will actually be equal to the result returned by an application of s. It merely tells us that *in principle* (in all possible executions) any result produced by t can also be produced by s and vice versa.

Equality in our view should be a *necessary* equality which must hold in every evaluation of a program (specification). *It does not correspond to set equality but to identity of one-element sets.* Thus the simple formula $\mapsto t = s$ will hold in a multistructure M iff both t and s are interpreted in M as one and the same set which, in addition, *has only one element.* Equality is then a *partial equivalence relation*, and terms t for which $\mapsto t = t$ holds are exactly the deterministic terms, denoted by $D_{SP,X}$. This last equality indicates that arbitrary two applications of t have to return the same result.

If it is possible to produce a computation where t and s return different results—and this is possible when they are nondeterministic—then the terms are not equal but, at best, *equivalent.* They are equivalent if they are capable of returning the same results, i.e., if they are interpreted as the same set. This may be expressed using the inclusion relation: $s \prec t$ holds iff the set of possible results of s is included in the set of possible results of t, and $s \asymp t$ if each is included in the other.

Having introduced inclusion one might expect that a nondeterministic operation can be specified by a series of inclusions, each defining one of its possible results. However, such a specification gives only a "lower bound" on the admitted nondeterminism. Consider the following example.

Example 3.1.

S: {Nat},

F:

0:	$\to$ Nat	(zero)
$s\_$:	Nat $\to$ Nat	(successor)
$\_\sqcup\_$:	Nat $\times$ Nat $\to$ Nat	(binary nondeterministic choice)

Π:

(1) $\mapsto 0 = 0$	
(2) $\mapsto s(x) = s(x)$	
(3) $1 \frown 0 \mapsto$	(As usual), we abbreviate $s^n(0)$ as n.)
(4) $\mapsto 0 \prec 0 \sqcup 1 \qquad \mapsto 1 \prec 0 \sqcup 1$	

The first two axioms make zero and successor deterministic. A limited form of negation is present in $\mathcal{L}$ in the form of sequents with empty consequent. Axiom (3) makes 0 distinct from 1. Axioms (4) make then $\sqcup$ a nondeterministic choice with 0 and 1 among its possible results. This, however, ensures only that in every model both 0 and 1 can be returned by $0 \sqcup 1$. In most models all other kinds of elements may be among its possible results as well, since no extension of the result set of $0 \sqcup 1$ will violate the inclusions of (4). If we are satisfied with this degree of precision, we may stop here and use only the Horn formula. All the results in the rest of the paper apply to this special case. But to specify an "upper bound" of nondeterministic operations we need *disjunction*, the multiple formulas in the consequents. Now, if we write the axiom

(5) $\mapsto 0 \sqcup 1 = 0, \quad 0$

the two occurrences of $0 \sqcup 1$ r
obtain that either any applica
not really nondeterministic bu
both 0 and 1 be among the
specification inconsistent.

What we are trying to say
$0 \sqcup 1$ returns either 0 or 1; i.e
nondeterministic term as refer
by *binding* both occurrences t

(5′) $x \frown 0 \sqcup 1 \mapsto x =$

The axiom says: whenever $0 \sqcup$
such an interpretation presupp
value. Thus bindings have the i
(Plural variables, on the other
axiom

(5″) $x^* \frown 0 \sqcup 1 \mapsto x^*$

would have a completely diffe
common in the literature on
languages [2, 8, 11], in spite of
terms for variables. Any subs
substituted term yields a uniqu
in the subsection on reasoning,
one, for instance, to conclude 0
(though it could be obtained fr

4. The singular case:
multialgebraic semantics of spe
sound and complete calculus.

4.1. Multistructures an

DEFINITION 4.2 (Multistruc
if

(1) *its carrier* |M| *is an* **S**-
(2) *for every* f: $S_1 \times \cdots \times$
f^M: $S_1^M \times \cdots \times S_n^M \to$

A function $\mathbf{\Phi}$: A $\to$ B *(i.e., a fa*
multihomomorphism *from a* Σ-
(H1) *for each constant sym*
(H2) *for every* f: $S_1 \times \cdots$
$\mathbf{\Phi}(f^A(\underline{a}_1 \cdots \underline{a}_n)) \subseteq f^B$

If all inclusions in H1 *and* H2 *a*
wise it is strictly loose (or just l

$\mathcal{P}^+(S)$ denotes the set of no
sets refer to their unique pointw
indicates that c^M can be a *set* of

Since multihomomorphisms
serve singletons and are $\subseteq$-mono

(5) $\mapsto 0 \sqcup 1 = 0, \quad 0 \sqcup 1 = 1,$

the two occurrences of $0 \sqcup 1$ refer to two arbitrary applications and, consequently, we obtain that either any application of $0 \sqcup 1$ equals 0 or else it equals 1, i.e., that $\sqcup$ is not really nondeterministic but merely underspecified. Since axioms (4) require that both 0 and 1 be among the results of t, the addition of (5) will actually make the specification inconsistent.

What we are trying to say with the disjunction of (5) is that *every application* of $0 \sqcup 1$ returns either 0 or 1; i.e., we need a means of identifying two occurrences of a nondeterministic term as referring to one and the same application. This can be done by *binding* both occurrences to a variable. The appropriate axiom will be

(5′) $x \frown 0 \sqcup 1 \mapsto x = 0,\ x = 1.$

The axiom says: whenever $0 \sqcup 1$ returns x, then x equals 0 or x equals 1. Notice that such an interpretation presupposes that the variable x refers to a *unique, individual* value. Thus bindings have the intended function only if they involve *singular* variables. (Plural variables, on the other hand, will refer to sets and not individuals, and so the axiom

(5″) $x^* \frown 0 \sqcup 1 \mapsto x^* = 0,\ x^* = 1$

would have a completely different meaning.) The singular semantics is the most common in the literature on algebraic semantics of nondeterministic specification languages [2, 8, 11], in spite of the fact that it prohibits unrestricted substitution of terms for variables. Any substitution must now be guarded by the check that the substituted term yields a unique value, i.e., is deterministic. We return to this point in the subsection on reasoning, where we introduce a calculus which does not allow one, for instance, to conclude $0 \sqcup 1 = 0 \sqcup 1 \mapsto 0 \sqcup 1 = 0,\ 0 \sqcup 1 = 1$ from the axiom (5′) (though it could be obtained from (5″)).

4. The singular case: Semantics and calculus. This section defines the multialgebraic semantics of specifications with singular arguments and introduces a sound and complete calculus.

4.1. Multistructures and multimodels.

DEFINITION 4.2 (Multistructures). *Let* Σ *be a signature.* M *is a* Σ-multistructure *if*

(1) *its carrier* $|\mathrm{M}|$ *is an* $\mathbf{S}$*-sorted set,*
(2) *for every* $f\colon \mathrm{S}_1 \times \cdots \times \mathrm{S}_n \to \mathrm{S}$ *in* $\mathbf{F}$*, there is a corresponding function* $f^M\colon \mathrm{S}_1^{\mathrm{M}} \times \cdots \times \mathrm{S}_n^{\mathrm{M}} \to \mathcal{P}^+(\mathrm{S}^{\mathrm{M}})$.

A function $\mathbf{\Phi}\colon \mathrm{A} \to \mathrm{B}$ *(i.e., a family of functions* $\mathbf{\Phi}_{\mathrm{S}}\colon \mathrm{S}^{\mathrm{A}} \to \mathrm{S}^{\mathrm{B}}$ *for every* $\mathrm{S} \in \mathbf{S}$*) is a* multihomomorphism *from a* Σ*-multistructure* A *to* B *if*

(H1) *for each constant symbol* $c \in \mathbf{F}$, $\mathbf{\Phi}(c^A) \subseteq c^B$,
(H2) *for every* $f\colon \mathrm{S}_1 \times \cdots \times \mathrm{S}_n \to \mathrm{S}$ *in* $\mathbf{F}$ *and* $\underline{a}_1 \cdots \underline{a}_n \in \mathrm{S}_1^{\mathrm{A}} \times \cdots \times \mathrm{S}_n^{\mathrm{A}}$: $\mathbf{\Phi}(f^{\mathrm{A}}(\underline{a}_1 \cdots \underline{a}_n)) \subseteq f^{\mathrm{B}}(\mathbf{\Phi})(\underline{a}_i) \cdots \mathbf{\Phi}(\underline{a}_n))$.

If all inclusions in H1 *and* H2 *are (set) equalities the homomorphism is* tight*; otherwise it is strictly loose (or just* loose*).*

$\mathcal{P}^+(S)$ denotes the set of nonempty subsets of the set S. Operations applied to sets refer to their unique pointwise extensions. Notice that for a constant $c\colon \to S(2)$ indicates that c^{M} can be a *set* of several elements of sort S.

Since multihomomorphisms are defined on individuals and not sets they preserve singletons and are $\subseteq$-monotonic. We denote the class of Σ-multistructures by

$\mathrm{MStr}(\Sigma)$. It has the distinguished word structure MW_Σ defined in the obvious way, where each ground term is interpreted as a singleton set. We will treat such singleton sets as terms rather than one-element sets (i.e., we do not take special pains to distinguish MW_Σ and W_Σ). MW_Σ is not an initial Σ-structure since it is deterministic and there can exist several homomorphisms from it to a given multistructure. We do not focus on the aspect of initiality and merely register the useful fact from [11].

LEMMA 4.3. *M is a Σ-multistructure iff for every set of variables X and assignment β: $X \to |\mathrm{M}|$, there exists a unique function $\beta[\_]$: $\mathrm{W}_{\Sigma,\mathrm{X}} \to \mathcal{P}^+(|\mathrm{M}|)$ such that*

(1) $\beta[x] = \{\beta(x)\}$,
(2) $\beta[c] = c^M$,
(3) $\beta[f(t_i)] = \cup\{f^M(y_i) \mid y_i \in \beta[t_i]\}$.

In particular, for $X = \emptyset$ there is a unique interpretation function (not a multihomomorphism) $\mathcal{I}$: $W_\Sigma \to \mathcal{P}^+(|M|)$ satisfying the last two points of this definition.

As a consequence of the definition of multistructures, all operations are $\subseteq$-monotonic, i.e., $\beta[s] \subseteq \beta[t] \Rightarrow \beta[f(s)] \subseteq \beta[f(t)]$. Notice also that assignment in the lemma (and in general whenever it is an assignment of elements from a multistructure) means assignment of individuals, not sets.

Next we define the class of *multimodels* of a specification.

DEFINITION 4.4 (Satisfiability). *A Σ-multistructure* M satisfies *an $\mathcal{L}(\Sigma)$ sequent* π

$$t_i \frown s_i \mapsto p_j = r_j, m_k \prec n_k,$$

written $\mathrm{M} \models \pi$ *iff for every β*: $\mathrm{X} \to \mathrm{M}$ *we have*

$$\bigwedge_i \beta[t_i] \cap \beta[s_i] \neq \emptyset \Rightarrow \bigvee_j \beta[p_j] \equiv \beta[r_j] \vee \bigvee_k \beta[m_k] \subseteq \beta[n_k],$$

where $\mathrm{A} \equiv \mathrm{B}$ *iff* A *and* B *are the same one-element set.*

An SP-multimodel *is a Σ-multistructure which satisfies all the axioms of SP. We denote the class of multimodels of SP by MMod(SP).*

The reason for using nonempty intersection (and not set equality) as the interpretation of $\frown$ in the antecedents is the same as using "elementwise" equality $\equiv$ in the consequents. Since we avoid set equality in the positive sense (in the consequents), the most natural negative form seems to be the one we have chosen. For deterministic terms this is the same as equality, i.e., deterministic antecedents correspond exactly to the usual (deterministic) conditions. For nondeterministic terms this reflects our interest in binding such terms: the sequent "$\ldots s \frown t \ldots \mapsto \ldots$" is equivalent to "$\ldots x \frown s,\ x \frown t \ldots \mapsto \ldots$." A binding "$\ldots x \frown t \ldots \mapsto \ldots$" is also equivalent to the more familiar "$\ldots x \in t \ldots \mapsto \ldots$," so the notation $s \frown t$ may be read as an abbreviation for the more elaborate formula with two $\in$ and a new variable x not occurring in the rest of the sequent.

For a justification of this, as well as other choices we have made here, the reader is referred to [24].

4.2. The calculus for singular semantics. In [24] we introduced the calculus NEQ which is sound and complete with respect to the class MMod(SP). Its rules are as follows:

(R1) $\quad \mapsto x = x, \qquad x \in \mathcal{V},$

(R2) $\quad \dfrac{\boldsymbol{\Gamma}^x_{t_2} \mapsto \boldsymbol{\Delta}^x_{t_2} \quad ; \quad \boldsymbol{\Gamma}' \vdash}{\boldsymbol{\Gamma}^x_{t_1}, \boldsymbol{\Gamma}' \mapsto \boldsymbol{\Delta}^x_{t_1}}$

(R3) $\quad \dfrac{\boldsymbol{\Gamma}^x_{t_2} \mapsto \boldsymbol{\Delta}^x_{t_2} \quad ; \quad \boldsymbol{\Gamma}' \mapsto}{\boldsymbol{\Gamma}^x_{t_1}, \boldsymbol{\Gamma}' \mapsto \boldsymbol{\Delta}^x_{t_1}}$

(R4) $\quad$ (a) $x \frown y \mapsto x = y,$

(R5) $\quad \dfrac{\boldsymbol{\Gamma} \mapsto \boldsymbol{\Delta}, s \preceq t \quad ; \quad \boldsymbol{\Gamma}',}{\boldsymbol{\Gamma}, \boldsymbol{\Gamma}' \mapsto \boldsymbol{\Delta},}$

(R6) $\quad$ (a) $\dfrac{\boldsymbol{\Gamma} \mapsto \boldsymbol{\Delta}}{\boldsymbol{\Gamma} \mapsto \boldsymbol{\Delta}, e},$ $\qquad$ (b

(R7) $\quad \dfrac{\boldsymbol{\Gamma}, x \frown t \mapsto \boldsymbol{\Delta}}{\boldsymbol{\Gamma}^x_t \mapsto \boldsymbol{\Delta}^x_t},$ $\qquad x \in$

$\boldsymbol{\Gamma}^{\mathrm{a}}_{\mathrm{b}}$ denotes $\boldsymbol{\Gamma}$ with b substitute
in order.

The fact that "=" is a part
only to variables and is sound
(singular) variables.

(R2) is a paramodulation
terministic (in the case where t
it allows derivation of the stand
deterministic and prevents subs

(R3) allows "specialization"
term t_1 which is included in t_2.
substituted for don't occur in
unsound conclusion $\mapsto t_3 \prec t_1$ fi

(R4) and (R5) express the r
and inclusion in the consequent.
$s \frown t \mapsto s \preceq t$) does not hold in
nonempty intersection of the res
identity of one-element (=) resu
variables) s, t do we have that s

(R5) allows us to cut both $\vdash$

(R7) eliminates redundant b
term occurring at most once in t

We will write $\Pi \vdash_{\mathrm{CAL}} \boldsymbol{\pi}$ to i
CAL.

The counterpart of soundness
[24].

THEOREM 4.5. *NEQ is soun*

MMod(

Proof idea. Soundness is prov
$\boldsymbol{\pi}$. The proof of the completeness
style argument. The axiom set $\boldsymbol{\Pi}$

(R2) $$\frac{\Gamma^x_{t_2} \mapsto \Delta^x_{t_2} \quad ; \quad \Gamma' \mapsto t_1 = t_2, \Delta'}{\Gamma^x_{t_1}, \Gamma' \mapsto \Delta^x_{t_1}, \Delta'},$$

(R3) $$\frac{\Gamma^x_{t_2} \mapsto \Delta^x_{t_2} \quad ; \quad \Gamma' \mapsto t_1 \prec t_2, \Delta'}{\Gamma^x_{t_1}, \Gamma' \mapsto \Delta^x_{t_1}, \Delta'}, \quad x \text{ not in a RHS of } \prec,$$

(R4) (a) $x \frown y \mapsto x = y$, (b) $x \frown t \mapsto x \prec t$, $x, y \in \mathcal{V}$,

(R5) $$\frac{\Gamma \mapsto \Delta, s \preceq t \quad ; \quad \Gamma', s \frown t \mapsto \Delta'}{\Gamma, \Gamma' \mapsto \Delta, \Delta'}, \quad \text{(CUT)} \quad (\preceq \text{ stands for either } = \text{ or } \prec),$$

(R6) (a) $$\frac{\Gamma \mapsto \Delta}{\Gamma \mapsto \Delta, e}, \qquad \text{(b)} \quad \frac{\Gamma \mapsto \Delta}{\Gamma, e \mapsto \Delta} \qquad \text{(WEAK)},$$

(R7) $$\frac{\Gamma, x \frown t \mapsto \Delta}{\Gamma^x_t \mapsto \Delta^x_t}, \qquad x \in \mathcal{V} - \mathcal{V}[t], \text{ at most one } x \text{ in } \Gamma \mapsto \Delta \qquad \text{(ELIM)}.$$

Γ^a_b denotes Γ with b substituted for a. Short comments on each of the rules may be in order.

The fact that "=" is a partial equivalence relation is expressed in (R1). It applies only to variables and is sound because all assignments assign individual values to the (singular) variables.

(R2) is a paramodulation rule allowing replacement of terms which may be deterministic (in the case where $t_1 = t_2$ holds in the second assumption). In particular, it allows derivation of the standard substitution rule when the substituted terms are deterministic and prevents substitution of nondeterministic terms for variables.

(R3) allows "specialization" of a sequent by substituting for a term t_2 another term t_1 which is included in t_2. The restriction that the occurrences of t_2 which are substituted for don't occur in the RHS of $\prec$ is needed to prevent, for instance, the unsound conclusion $\mapsto t_3 \prec t_1$ from the premises $\mapsto t_3 \prec t_2$ and $\mapsto t_1 \prec t_2$.

(R4) and (R5) express the relation between $\frown$ in the antecedent and the equality and inclusion in the consequent. The axiom of standard sequent calculus, $e \mapsto e$, (i.e., $s \frown t \mapsto s \preceq t$) does not hold in general here because the antecedent corresponds to nonempty intersection of the result sets while the consequent to the inclusion ($\prec$) or identity of one-element ($=$) result sets. Only for deterministic terms (in particular, variables) s, t do we have that $s \frown t \mapsto s = t$ holds.

(R5) allows us to cut both $\mapsto s = t$ and $\mapsto s \prec t$ with $s \frown t \mapsto \Delta$.

(R7) eliminates redundant bindings, namely those that bind an application of a term occurring at most once in the rest of the sequent.

We will write $\Pi \vdash_{\text{CAL}} \pi$ to indicate that π is provable from Π with the calculus CAL.

The counterpart of soundness/completeness of the equational calculus is as follows [24].

THEOREM 4.5. *NEQ is sound and complete with respect to MMod(SP):*

$$\textit{MMod(SP)} \models \pi \textit{ iff } \Pi \vdash_{NEQ} \pi.$$

Proof idea. Soundness is proved by induction on the length of the proof $\Pi \vdash_{\text{NEQ}} \pi$. The proof of the completeness part is a standard, albeit rather involved, Henkin-style argument. The axiom set Π of SP is extended by adding all $\mathcal{L}(\text{SP})$ formulas π

which are consistent with $\mathbf{\Pi}$ (and the previously added formulas). If the addition of $\boldsymbol{\pi}$ leads to inconsistency, one adds the negation of $\boldsymbol{\pi}$. Since empty consequents provide only a restricted form of negation, the general negation operation is defined as a set of formulas over the original signature extended with new constants. One shows then that the construction yields a consistent specification with a deterministic basis from which a model can be constructed.

We also register an easy lemma that the set-equivalent terms $t \asymp s$ satisfy the same formulas.

LEMMA 4.6. *$t \asymp s$ iff, for any sequent $\boldsymbol{\pi}$, $\mathbf{\Pi} \vdash_{NEQ} \boldsymbol{\pi}^z_t$ iff $\mathbf{\Pi} \vdash_{NEQ} \boldsymbol{\pi}^z_s$.* □

5. The plural case: Semantics and calculus. The singular semantics for passing nondeterminate arguments is the most common notion to be found in the literature. Nevertheless, the plural semantics has also received some attention. In the denotational tradition most approaches considered both possibilities [18, 19, 20, 22]. Engelfriet and Schmidt gave a detailed study of both—in their language, IO and OI—semantics based on tree languages [5] and continuous algebras of relations and power sets [6]. The unified algebras of Mosses [17] and the rewriting logic of Meseguer [15] represent other algebraic approaches distinguishing these aspects.

We will define the semantics for specifications where operations may have both singular and plural arguments. The next subsection gives the necessary extension of the calculus NEQ to handle this generalized situation.

5.1. Power structures and power models. Singular arguments (such as the variables in $\mathcal{L}$) have the usual algebraic property that they refer to a unique value. This reflects the fact that they are evaluated at the moment of substitution and the result is passed to the following computation. Plural arguments, on the other hand, are best understood as textual parameters. They are not passed as a single value, but every occurrence of the formal parameter denotes a distinct application of the operation.

We will allow both singular and plural parameter passing in one specification. The corresponding semantic distinction is between power set functions which are merely $\subseteq$-monotonic and those which also are $\cup$-additive.

In the language, we merely introduce a notational device for distinguishing the singular and plural arguments. We allow annotating the sorts in the profiles of the operation by a superscript, like S^*, to indicate that an argument is plural.

Furthermore, we partition the set of variables into two disjoint subsets of singular X and plural X^* variables. x and x^* are to be understood as distinct symbols. We will say that an operation f is *singular in the ith argument* iff the ith argument (in its signature) is singular. The specification language extended with such annotations of the signatures will be referred to as $\mathcal{L}^*$.

These are the only extensions of the language we need. We may, optionally, use superscripts t^* at any (sub)term to indicate that it is passed as a plural argument. The outermost applications, e.g., f in $f(\ldots)$, are always to be understood plurally, and no superscripting will be used at such places.

DEFINITION 5.1. *Let Σ be a $\mathcal{L}^*$-signature. A is a* Σ-power structure $A \in PStr(\Sigma)$ *iff A is a (deterministic) structure such that*

1. *for every sort* S, *the carrier* S^{A} *is a (subset of the) power set* $\mathcal{P}^+(\mathrm{S}^-)$ *of some basis set* S^-,
2. *for every* $f\colon \mathrm{S}_1 \times \cdots \times \mathrm{S}_n \to \mathrm{S}$ *in* Σ, f^A *is a* $\subseteq$*-monotonic function* $\mathrm{S}_1^{\mathrm{A}} \times \cdots \times \mathrm{S}_n^{\mathrm{A}} \to \mathrm{S}^{\mathrm{A}}$ *such that if the ith argument is* S_i *(singular), then* f^A *is singular in the ith argument.*

The singularity in the ith
notion but to its semantic cou
DEFINITION 5.2. *A funct*
singular in the ith argument
$x_i \in \mathrm{S}_i^{\mathrm{A}}$ *and all* $x_k \in \mathrm{S}_k^{\mathrm{A}}$ *(for*
$x \in x_i\}$.

Thus, the definition of p
modeled by the semantic one.

Note the unorthodox point
whole power set but allow it t
primitive nondeterministic ope
all finite subsets are needed f
the join operation (under the s
union only if all sets are prese
necessary. Consequently, we
instead, give the user means o
choice) directly.

Let Σ be a signature, A a
X^* a set of plural variables,
$x \in X : |\boldsymbol{\beta}(x)| = 1$. (Saying as
satisfying this last condition.)
interpretation $\beta[t(x, x^*)]$ in A

DEFINITION 5.3 (Satisfiab
$p_j = r_j$, $m_k \prec n_k$ *be a sequent*
assignment $\boldsymbol{\beta}$: $X \cup X^* \to |A|$,

$$\bigwedge_i \boldsymbol{\beta}[t_i] \cap \boldsymbol{\beta}[s_i] \neq$$

A *is a* power model *of the speci*
and A satisfies all axioms from

Except for the change in th
4.4, which is the reason for ret

5.2. The calculus for
with one additional rule:

$$\text{(R8)} \quad \frac{\mathbf{\Gamma} \mapsto \mathbf{\Delta}}{\mathbf{\Gamma}^{x^*}_t \mapsto \mathbf{\Delta}^{x^*}_t}.$$

Rules (R1)–(R7) remain unch
particular, any t_i may be a plu
R8.

The new rule (R8) expres
substitute an arbitrary term t
variable x, we can thus exchang
ones. The opposite is, in gen
singular variables. For instance
is not sufficient for performing
main result concerning PMod a

THEOREM 5.4. *For any $\mathcal{L}^*$*

PMo

The singularity in the ith argument in this definition refers not to the syntactic notion but to its semantic counterpart.

DEFINITION 5.2. *A function* f^A: $\mathrm{S}_1^{\mathrm{A}} \times \cdots \times \mathrm{S}_n^{\mathrm{A}} \to \mathrm{S}^{\mathrm{A}}$ *in a power structure* A *is* singular in the ith argument *iff it is* $\cup$*-additive in the* i*th argument, i.e., iff for all* $x_i \in \mathrm{S}_i^{\mathrm{A}}$ *and all* $x_k \in \mathrm{S}_k^{\mathrm{A}}$ *(for* $k \neq i$*),* $f^A(x_1 \cdots x_i \cdots x_n) = \cup\{f^A(x_1 \cdots \{x\} \cdots x_n) \mid x \in x_i\}$.

Thus, the definition of power structures requires that syntactic singularity be modeled by the semantic one.

Note the unorthodox point in the definition: we do not require the carrier to be the whole power set but allow it to be a *subset* of some power set. Usually one assumes a primitive nondeterministic operation with the predefined semantics as set union. Then all finite subsets are needed for the interpretation of this primitive operator. Also, the join operation (under the set inclusion as partial order) corresponds exactly to set union only if all sets are present (see Example 6.8). None of these assumptions seem necessary. Consequently, we do not assume any predefined (choice) operation but, instead, give the user means of specifying any nondeterministic operation (including choice) directly.

Let Σ be a signature, A a Σ-power structure, X a set of singular variables and X^* a set of plural variables, and $\boldsymbol{\beta}$ an assignment $X \cup X^* \to |A|$ such that for all $x \in X : |\boldsymbol{\beta}(x)| = 1$. (Saying assignment we will from now on mean only assignments satisfying this last condition.) Then, every term $t(x, x^*) \in W_{\Sigma,\mathrm{X},\mathrm{X}^*}$ has a unique set interpretation $\beta[t(x, x^*)]$ in A defined as $t^A(\boldsymbol{\beta}(x), \boldsymbol{\beta}(x^*))$.

DEFINITION 5.3 (Satisfiability). *Let* A *be a* Σ*-power structure and* $\boldsymbol{\pi}$: $t_i \frown s_i \mapsto p_j = r_j,\ m_k \prec n_k$ *be a sequent over* $\mathcal{L}^*(\Sigma, X, X^*)$. A satisfies $\boldsymbol{\pi}$, $A \models \pi$, *iff for every assignment* $\boldsymbol{\beta}$: $X \cup X^* \to |A|$, *we have that*

$$\bigwedge_i \boldsymbol{\beta}[t_i] \cap \boldsymbol{\beta}[s_i] \neq \emptyset \Rightarrow \bigvee_j \boldsymbol{\beta}[p_j] \equiv \boldsymbol{\beta}[r_j] \vee \bigvee_k \boldsymbol{\beta}[m_k] \subseteq \boldsymbol{\beta}[n_k].$$

A *is a* power model *of the specification* $\mathrm{SP} = (\Sigma, \boldsymbol{\Pi})$, $A \in PMod(SP)$, *iff* $A \in \mathrm{PStr}(\Sigma)$ *and* A *satisfies all axioms from* $\boldsymbol{\Pi}$.

Except for the change in the notion of an assignment, this is identical to Definition 4.4, which is the reason for retaining the same notation for the satisfiability relation.

5.2. The calculus for plural parameters. The calculus NEQ is extended with one additional rule:

$$\text{(R8)} \qquad \frac{\boldsymbol{\Gamma} \mapsto \boldsymbol{\Delta}}{\boldsymbol{\Gamma}_t^{x^*} \mapsto \boldsymbol{\Delta}_t^{x^*}}.$$

Rules (R1)–(R7) remain unchanged, but now all terms t_i belong to $W_{\Sigma,\mathrm{X},\mathrm{X}^*}$. In particular, any t_i may be a plural variable. We let NEQ* denote the calculus NEQ + R8.

The new rule (R8) expresses the semantics of plural variables. It allows us to substitute an arbitrary term t for a plural variable x^*. Taking t to be a singular variable x, we can thus exchange plural variables in a provable sequent $\boldsymbol{\pi}$ with singular ones. The opposite is, in general, not possible because rule (R1) applies only to singular variables. For instance, a plural variable x^* will satisfy $\mapsto x^* \prec x^*$, but this is not sufficient for performing a general substitution for a singular variable. The main result concerning PMod and NEQ* is as follows.

THEOREM 5.4. *For any* $\mathcal{L}^*$*-specification SP and* $\mathcal{L}^*$*(SP) sequent* $\boldsymbol{\pi}$:

$$PMod(SP) \models \boldsymbol{\pi} \text{ iff } \boldsymbol{\Pi} \vdash_{NEQ^*} \boldsymbol{\pi}.$$

Proof idea. The proof is a straightforward extension of the proof of Theorem 4.5. □

6. Comparison. Since plural and singular semantics are certainly not one and the same thing, it may seem surprising that essentially the same calculus can be used for reasoning about both. One would perhaps expect that PMod, being a richer class than MMod, will satisfy fewer formulas than the latter and that some additional restrictions of the calculus would be needed to reflect the increased generality of the model class. In this section we describe precisely the relation between the $\mathcal{L}$ and $\mathcal{L}^*$ specifications (section 6.1) and emphasize some points of difference (section 6.2).

6.1. The "equivalence" of both semantics. The following example illustrates a strong sense of equivalence of $\mathcal{L}$ and $\mathcal{L}^*$.

Example 6.1. Consider the following plural definition:

$$\mapsto f(x^*) \prec \text{ if } x^* = x^* \text{ then } 0 \text{ else } 1.$$

It is "equivalent" to the collection of definitions

$$\mapsto f(t) \prec \text{ if } t = t \text{ then } 0 \text{ else } 1$$

for all terms t.

In the rest of this section we will clarify the meaning of this "equivalence."

Since the partial order of functions from a set A to the power set of a set B is isomorphic to the partial order of additive (and strict, if we take $\mathcal{P}$ (all subsets) instead of $\mathcal{P}^+$) functions from the power set of A to the power set of B, $[A \to \mathcal{P}(B)] \simeq [\mathcal{P}(A) \to_\cup \mathcal{P}(B)]$, we may consider every multistructure A to be a power structure A^* by taking $|A^*| = \mathcal{P}^+(A)$ and extending all operations in A pointwise. We then have the obvious lemma.

LEMMA 6.2. *Let SP be a singular specification (i.e., all operations are singular in all arguments), let* $A \in \mathrm{MStr(SP)}$, *and let* π *be a sequent in* $\mathcal{L}(\mathrm{SP})$. *Then* $A \models \pi$ *iff* $A^* \models \pi$, *and so* $A \in MMod(SP)$ *iff* $A^* \in PMod(SP)$.

Call an $\mathcal{L}^*$ sequent π *p-ground* (for plurally ground) if it does not contain any plural variables.

THEOREM 6.3. *Let* $\mathrm{SP}^* = (\Sigma^*, \mathbf{\Pi}^*)$ *be an* $\mathcal{L}^*$ *specification. There exists a (usually infinite)* $\mathcal{L}$ *specification* $\mathrm{SP} = (\Sigma, \mathbf{\Pi})$ *such that*

(1) $W_{\Sigma,\mathrm{X}} = W_{\Sigma^*,\mathrm{X}}$

(2) *for any* p-*ground* $\pi \in \mathcal{L}^*(\mathrm{SP}^*) : \mathrm{PMod}(\mathrm{SP}^*) \models \pi$ iff $\mathrm{MMod}(\mathrm{SP}) \models \pi$.

Proof. Let Σ be Σ^* with all "*" symbols removed. This makes (1) true. Any p-ground π as in (2) is then a π over the language $\mathcal{L}(\Sigma, X)$.

The axioms $\mathbf{\Pi}$ are obtained from $\mathbf{\Pi}^*$ as in Example 6.1. For every $\pi^* \in \mathbf{\Pi}^*$ with plural variables $x_1^* \cdots x_n^*$, let $\pi = \{\pi^* \begin{smallmatrix} x_1^* \cdots x_n^* \\ t_1 \cdots t_n \end{smallmatrix} \mid t_1 \cdots t_n \in W_{\Sigma,\mathrm{X}}\}$. Obviously, for any $\pi \in \mathcal{L}(\mathrm{SP})$ if $\mathbf{\Pi} \vdash_{\mathrm{NEQ}} \pi$ then $\mathbf{\Pi}^* \vdash_{\mathrm{NEQ}^*} \pi$. If $\mathbf{\Pi}^* \vdash_{\mathrm{NEQ}^*} \pi$ then the proof can be simulated in NEQ. Let $\pi'(x^*)$ be the last sequent used in the NEQ*-proof which contains plural variables x^* and the sequent π' be the next one obtained by (R8). Build the analogous NEQ-proof tree with all plural variables replaced by the terms which occupy their place in π'. The leaves of this tree will be instances of the $\mathbf{\Pi}^*$ axioms with plural variables replaced by the appropriate terms, and all such axioms are in $\mathbf{\Pi}$. Then soundness and completness of NEQ and NEQ* imply the conclusion of the theorem. □

We now ask whether, or under which conditions, the classes PMod and MMod are interchangeable as the models of a specification. Let SP*, SP be as in the theorem. The one-way transition is trivial. Axioms of SP are p-ground, so PMod(SP*) will satisfy all these axioms by the theorem. The subclass $\downarrow$ PMod(SP*) $\subseteq$ PMod(SP*), where for every P $\in\downarrow$ PMod(SP*) all operations are singular, will yield a subclass of MMod(SP).

For the other direction, we have to observe that the restriction to p-ground sequents in the theorem is crucial because plural variables range over arbitrary, also undenotable, sets. Let MMod*(SP) denote the class of power structures obtained as in Lemma 6.2. It is not necessarily the case that MMod*(SP) $\models \mathbf{\Pi}^*$, as the following argument illustrates.

Example 6.4. Let $M^* \in$ MMod*(SP) have infinite carrier, $\boldsymbol{\pi}^* \in \mathbf{\Pi}^*$ be $t_i \frown s_i \mapsto p_j = r_j$, $m_k \prec n_k$ with $x^* \in \mathcal{V}[\boldsymbol{\pi}^*]$, and $\boldsymbol{\beta}$: $X \cup X^* \to |M^*|$ be an assignment such that $\boldsymbol{\beta}(x^*) = \{\underline{m}_1 \cdots \underline{m}_l \cdots\}$ is a set which is not denoted by any term in $W_{\Sigma,\mathrm{X}}$. Let $\boldsymbol{\beta}_l$ be an assignment equal to $\boldsymbol{\beta}$ except that $\boldsymbol{\beta}_l(x^*) = \{\underline{m}_l\}$, i.e., $\boldsymbol{\beta} = \cup_l \boldsymbol{\beta}_l$. Then $M^* \models \boldsymbol{\beta}[\boldsymbol{\pi}^*]$ iff

$$M^* \models \boldsymbol{\beta}[t_i] \cap \boldsymbol{\beta}[s_i] \neq \emptyset \Rightarrow \boldsymbol{\beta}[p_j] \equiv \boldsymbol{\beta}[r_j] \vee \ldots \vee \boldsymbol{\beta}[m_k] \subseteq \boldsymbol{\beta}[n_k] \quad \text{iff}$$

$$\text{(a)}\ M^* \models \bigcup_l \boldsymbol{\beta}_l[t_i] \cap \bigcup_l \boldsymbol{\beta}_l[s_l] \neq \emptyset \Rightarrow \bigcup_l \boldsymbol{\beta}_l[p_j] \equiv \bigcup_l \boldsymbol{\beta}_l[r_j] \vee \ldots \vee \bigcup_l \boldsymbol{\beta}_l[m_k] \subseteq \bigcup_l \boldsymbol{\beta}_l[n_k]$$

since operations in M^* are defined by pointwise extension. $M^* \in$ MMod*(SP) implies that, for all l

$$\text{(b)}\ M^* \models \boldsymbol{\beta}_l[t_i] \cap \boldsymbol{\beta}_l[s_l] \neq \emptyset \Rightarrow \boldsymbol{\beta}_l[p_j] \equiv \boldsymbol{\beta}_l[r_j] \vee \ldots \vee \boldsymbol{\beta}_l[m_k] \subseteq \boldsymbol{\beta}_l[n_k].$$

But (b) does not necessarily imply (a). In particular, even if for all l, all intersections in the antecedent of (b) are empty, those in (a) may be nonempty. So we are not guaranteed that $M^* \in$ PMod(SP*).

Thus, the intuition that the multimodels are contained in the power models is not quite correct. To ensure that no undenotable sets from M^* can be assigned to the plural variables we redefine the lifting operator *: MMod(SP) $\to$ PMod(SP) from Lemma 6.2.

DEFINITION 6.5. *Given a singular specification SP and $M \in MMod(SP)$, we denote by* $\uparrow$M *the following power structure:*

(1) $|\uparrow \mathrm{M}| \subseteq \mathcal{P}^+(|\mathrm{M}|)$ *is such that*

(a) *for every* $\underline{n} \in |M|$: $\{\underline{n}\} \in |\uparrow \mathrm{M}|$,

(b) *for every* $\underline{m} \in |\uparrow \mathrm{M}|$ *there exists a* $t \in W_{\Sigma,\mathrm{X}}$, $\underline{n} \in |\mathrm{M}|$ *such that:* $t^M(\underline{n}) = \underline{m}$.

(2) *The operations in* $\uparrow$M *can be then defined by:* $f(\underline{m})^{\uparrow M} = f(t(\underline{n}))^M$.

Then, for any assignment $\boldsymbol{\beta}$: $X^* \to |\uparrow \mathrm{M}|$ there exists an assignment $\boldsymbol{\theta}$: $X^* \to W_{\Sigma,\mathrm{X}}$ (1b) and an assignment $\boldsymbol{\alpha}$: $X \to |M|$ (1a) such that $\boldsymbol{\beta}(x^*) = \boldsymbol{\alpha}\boldsymbol{\theta}(x^*)]$ (2), i.e., such that the diagram in Figure 1 commutes.

Since $M \in$ MMod(SP), it satisfies all the axioms $\mathbf{\Pi}$ obtained from $\mathbf{\Pi}^*$ and the commutativity of the figure gives us the second part of the following.

COROLLARY 6.6. *Let SP* and SP be as in Theorem* 6.3. *Then*

$$\downarrow PMod(SP^*) \models \mathbf{\Pi},\ \textit{i.e.,}\ \downarrow PMod(SP^*) \subseteq MMod(SP),$$
$$\uparrow MMod(SP) \models \mathbf{\Pi}^*,\ \textit{i.e.,}\ \uparrow MMod(SP) \subseteq PMod(SP^*).$$

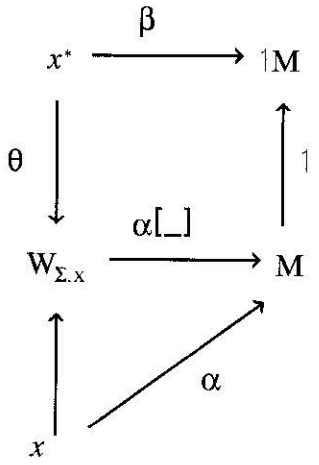

FIG. 1.

The corollary makes precise the claim that the class of power models of a plural specification SP* may be seen as a class of multimodels of some singular specification SP and vice versa. The reasoning about both semantics is essentially the same because the only difference concerns the (arbitrary) undenotable sets which can be referred to by plural variables.

6.2. Plural specification of choice. Plural variables provide access to arbitrary sets. In the following example we attempt to utilize this fact to give a more concise form to the specification of choice.

Example 6.7. The specification

S: $\{ \mathrm{S} \}$,
F: $\{ \sqcup\_ : \mathrm{S}^* \to \mathrm{S} \}$,
Π: $\{ \mapsto \sqcup . x^* \asymp x^* \}$

defines $\sqcup$. as the choice operator: for any argument t, $\sqcup . t$ is capable of returning any element belonging to the set interpreting t.

The specification may seem plausible, but there are several difficulties. Obviously, such a choice operation would be redundant in any specification since the axiom makes $\sqcup . t$ observationally equivalent to t, and Lemma 4.6 allows us to remove any occurrences of $\sqcup$. from the (derivable) formulas. Furthermore, observe how such a specification confuses the issue of nondeterministic choice. Choice is supposed to take a *set* as an argument and return *one element* from the set or, perhaps, to convert an argument of type "set" to a result of type "individual." This is the intention behind writing the specification above. But power algebras model all operations as functions on power sets and such a "conversion" simply does not make sense. The only points where conversion of a set to an individual takes place is when a term is passed as a singular argument to another operation. If we have an operation with a singular argument f: $\mathrm{S} \to \mathrm{S}$, then $f(t)$ will make (implicitly) the choice from t.

This might be particularly confusing because one tends to think of plural arguments as sets and mix up the semantic sets (i.e., the elements of the carrier of a power algebra) and the syntactic ones (as expressed by the profiles of the operations in the

R8 $x \frown z^*, y \frown z^* \mapsto$
R7 $x \frown p, y \frown p \mapsto$
R7 $y \frown p \mapsto p \sqcup$
$\mapsto p \sqcup p \prec$

signature). As a matter of fa
intention of choosing an eleme
choice the signature $Set(S)$ –
$\mathcal{P}^+(Set(S))$ to $\mathcal{P}^+(S)$. Assun
to the power set construction,
with a power set of a power s
we cannot let the same variab

Example 6.7 and remarks
standing of plural parameters.
significantly complicate the mo

On the other hand, plura
nondeterministic choice witho
ified as the join which under
correspond to set union (cf. [1

Example 6.8. The followi
wrt. $\prec$:

S: $\{ \mathrm{S} \}$,
F: $\{ \_\sqcup\_ : \mathrm{S} \times \mathrm{S} \to \mathrm{S} \}$
Π: $\{$ (1) $\mapsto x^* \prec x^* \sqcup$
(2) $x \frown z^*, y \frown z$

Axiom (2) although using sing
with respect to all terms. (Not
would have a different, and in
whenever $\mapsto t \prec p$ and $\mapsto s \prec$
(see Figure 2). Violating our
shows the validity of the form
$s \prec p \mapsto t \sqcup s \prec p$.

Thus, in any model of the
then natural to consider $\sqcup$ as t
nondeterministic operations.
same as set union, we have to re
of the model. For instance, the

$\mathrm{S}^{\mathrm{A}} = \{ \{1\}, \{2\},$
$\sqcup^{\mathrm{A}}$ defined as x^*

will be a model of the specificat

7. Conclusion. We have c
choice) and plural (run-time-cho
the central results reported in t

$$\dfrac{\dfrac{\dfrac{x \frown z^*, y \frown z^* \mapsto x \sqcup y \prec z^*}{x \frown p, y \frown p \mapsto x \sqcup y \prec p}\,\text{R8}}{y \frown p \mapsto p \sqcup y \prec p}\,\text{R7}}{\mapsto p \sqcup p \prec p}\,\text{R7} \qquad \dfrac{\dfrac{\mapsto t \prec p \quad \mapsto p \sqcup p \prec p \sqcup p}{\mapsto t \sqcup p \prec p \sqcup p}\,\text{R3} \qquad \mapsto s \prec p}{\mapsto t \sqcup s \prec p \sqcup p}\,\text{R3}$$

$$\mapsto t \sqcup s \prec p \quad \text{R3}$$

FIG. 2.

signature). As a matter of fact, the above specification does not at all express the intention of choosing an element from the set. In order to do that it would have to give choice the signature $Set(S) \to S$. Semantically, this would then be a function from $\mathcal{P}^+(Set(S))$ to $\mathcal{P}^+(S)$. Assuming that semantics of $Set(S)$ will somehow correspond to the power set construction, this makes things rather complicated, forcing us to work with a power set of a power set. Furthermore, since $Set(S)$ and S are different sorts, we cannot let the same variable range over both as was done in the example above.

Example 6.7 and remarks illustrate some of the problems with the intuitive understanding of plural parameters. Power algebras, needed for modeling such parameters, significantly complicate the model of nondeterminism as compared with multialgebras.

On the other hand, plural variables allow us to specify the "upper bound" of nondeterministic choice without using disjunction. The choice operation can be specified as the join which under the partial ordering $\prec$ interpreted as set inclusion will correspond to set union (cf. [17]).

Example 6.8. The following specification makes binary choice the join operation wrt. $\prec$:

S: $\{ \mathrm{S} \}$,

F: $\{ \_\sqcup\_ : \mathrm{S} \times \mathrm{S} \to \mathrm{S} \}$,

Π: $\{$ (1) $\mapsto x^* \prec x^* \sqcup y^* \qquad \mapsto y^* \prec x^* \sqcup y^*$

(2) $x \frown z^*, y \frown z^* \mapsto x \sqcup y \prec z^*$ $\}$.

Axiom (2) although using singular variables x, y, does specify the minimality of $\sqcup$ with respect to all terms. (Notice that the axiom $x^* \frown z^*$, $y^* \frown z^* \mapsto x^* \sqcup y^* \prec z^*$ would have a different, and in this context unintended, meaning.) We can show that whenever $\mapsto t \prec p$ and $\mapsto s \prec p$ hold (for arbitrary terms) then so does $\mapsto t \sqcup s \prec p$ (see Figure 2). Violating our formalism a bit, we may say that the above proof shows the validity of the formula stating the expected minimality of join: $t \prec p$, $s \prec p \mapsto t \sqcup s \prec p$.

Thus, in any model of the specification from Example 6.8 $\sqcup$ will be a join. It is then natural to consider $\sqcup$ as the basic (primitive) operation used for defining other nondeterministic operations. Observe also that in order to ensure that join is the same as set union, we have to require the presence of *all* (finite) subsets in the carrier of the model. For instance, the power structure A with the carrier

$$\mathrm{S}^{\mathrm{A}} = \{ \{1\}, \{2\}, \{3\}, \{1,2,3\} \} \text{ and}$$

$\sqcup^{\mathrm{A}}$ defined as $x^{\mathrm{A}} \sqcup^{\mathrm{A}} y^{\mathrm{A}} = \{1,2,3\}$ whenever $x^{\mathrm{A}} \neq y^{\mathrm{A}}$

will be a model of the specification although $\sqcup^{\mathrm{A}}$ is not the same as set union.

7. Conclusion. We have defined the algebraic semantics for singular (call-time-choice) and plural (run-time-choice) passing of nondeterministic parameters. One of the central results reported in the paper is soundness and completeness of two new

reasoning systems NEQ and NEQ*, respectively, for singular and plural semantics. The plural calculus NEQ* is a minimal extension of NEQ which merely allows unrestricted substitution for plural variables. This indicated a close relationship between the two semantics. We have shown that plural specifications have equivalent (modulo undenotable sets) singular formulations if one considers the plural axioms as singular axiom schemata.

Acknowledgments. We are grateful to Manfred Broy for pointing out the inadequacy of our original notation and to Peter D. Mosses for the observation that in the presence of plural variables choice may be specified as join with Horn formulas.

REFERENCES

[1] J. A. Bergstra and J. W. Klop, *Algebra of communicating processes*, in Mathematics and Computer Science, CWI Monographs, 1, North-Holland, Amsterdam, 1986, pp. 89–138.
[2] W. Clinger, *Nondeterministic call by need is neither lazy nor by name, Proc. ACM Symposium on LISP and Functional Programming*, 1982, pp. 226–234.
[3] E. W. Dijkstra, *A discipline of Programming*, Prentice-Hall, Englewood Cliffs, NJ, 1976.
[4] H. Ehrig and B. Mahr, *Fundamentals of Algebraic Specification*, Vol. 1, Springer-Verlag, Berlin, 1985.
[5] J. Engelfriet and E. M. Schmidt, *IO and OI.* 1, J. Comput. System Sci., 15 (1977),pp. 328–353.
[6] J. Engelfriet and E. M. Schmidt, *IO and OI.* 2, J. Comput. System Sci., 16 (1978), pp. 67–99.
[7] J. A. Goguen and J. Meseguer, Completeness of Many-Sorted Equational Logic, *SIGPLAN Notices*, 17 (1982), pp. 9–17.
[8] M. C. B. Hennessy, *The semantics of call-by-value and call-by-name in a nondeterministic environment*, SIAM J. Comput., 9 (1980), pp. 67–84.
[9] C. A. R. Hoare, *Communicating Sequential Processes*, Prentice-Hall International Ltd., Englewood Cliffs, NJ, 1985.
[10] H. Hussmann, *Nondeterministic Algebraic Specifications*, Ph.D. thesis, Fakultät für Mathematik und Informatik, Universität Passau, 1990.
[11] H. Hussmann, *Nondeterminism in Algebraic Specifications and Algebraic Programs*, Birkhäuser, Basel, Switzerland, 1993.
[12] S. Kaplan, *Rewriting with a nondeterministic choice operator*, Theoret. Comput. Sci., 56 (1988), pp. 37–57.
[13] D. Kapur, *Towards a Theory of Abstract Data Types*, Ph.D. thesis, Laboratory for Computer Science, MIT, Cambridge, MA, 1980.
[14] S. Meldal, *An abstract axiomatization of pointer types*, in Proc. 22nd Annual Hawaii International Conference on System Sciences, IEEE Computer Society Press, Piscataway, NJ, 1989.
[15] J. Meseguer, *Conditional rewriting logic as a unified model of concurrency*, Theoret. Comput. Sci., 96 (1992), pp. 73–155.
[16] R. Milner, *Calculi for Communicating Systems*, Lecture Notes in Computer Science, Vol. 92, Springer-Verlag, Basel, Switzerland, 1980.
[17] P. D. Mosses, *Unified algebras and institutions*, in *Proc. LICS '89, Fourth Annual Symposium on Logic in Computer Science*, Pacific Grove, CA, 1989.
[18] C. E. S. Ore, *Introducing Girard's Quantitative Domains; the Quantitative Domains as a Model for Nondeterminism*, Ph.D. thesis, Dept. of Informatics, University of Oslo, Norway, 1988.
[19] G. Plotkin, Domains, 1983, Lecture notes, Dept. of Computer Science, University of Edinburgh, Scotland.
[20] H. Søndergaard and P. Sestoft, *Non-Determinacy and Its Semantics*, Technical report 86/12, Datalogisk Institut, Københavns Universitet, 1987.
[21] R. L. Schwartz, *An axiomatic treatment of ALGOL 68 routines*, in Proc. Sixth Colloquium on Automata, Languages and Programming, Vol. 71, Springer-Verlag, Basel, Switzerland, 1979.
[22] M. B. Smyth, *Power domains*, J. Comput. System Sci., 16 (1978), pp. 23 36.
[23] P. A. Subrahmanyam, *Nondeterminism in abstract data types*, in Automata, Languages and Programming, Lecture Notes in Computer Science, Vol. 115, Springer-Verlag, Basel,

Switzerland, 1981.
[24] M. Walicki, *Algebraic Spec*
matics, University of Be
[25] M. Walicki and S. Melda
and inclusions, in Rece
Science, Vol. 906, Spring
[26] G. Winskel, *An Introduct*
Vol. 354, Springer-Verla
[27] M. Wirsing, *Algebraic spec*
The MIT Press, Cambri

Switzerland, 1981.

[24] M. WALICKI, *Algebraic Specifications of Nondeterminism*, Ph.D. thesis, Department of Informatics, University of Bergen, 1993.

[25] M. WALICKI AND S. MELDAL, *Multialgebras, power algebras and complete calculi of identities and inclusions*, in Recent Trends in Data Type Specification, Lecture Notes in Computer Science, Vol. 906, Springer-Verlag, Basel, Switzerland, 1994.

[26] G. WINSKEL, *An Introduction to Event Structures*, Lecture Notes in Computer Science, Vol. 354, Springer-Verlag, Basel, Switzerland, 1988.

[27] M. WIRSING, *Algebraic specification*, in Handbook of Theoretical Computer Science, Vol. B, The MIT Press, Cambridge, MA, 1990.